Meru Networks MC3000 WLAN Controller with AP208 for Avaya 3631 Wireless Telephone Configuration Note and Deployment Guide

1 PRODUCT SUMMARY

Manufacturer:	Meru Networks: www.merunetworks.com	
Product(s):	WLAN Controllers	Access Points
	MC3000	AP208
RF technology:	Spread-spectrum direct sequence (DS)	
Radio:	2.4 – 2.484 GHz	
Antenna Diversity:	Rx Diversity	
Security:	WEP, WPA-PSK, WPA2-PSK, WPA-802.1X, WPA2-802.1X	
AP software version:	3.2 SR1	
Recommended network topology:	Switched Ethernet (required)	

2 DEPLOYMENT SCENARIOS

Avaya 3631 Wireless telephones can be deployed in a Meru Networks WLAN system where the access points are deployed within a subnet or across multiple layer 2 subnets.

When deploying the system, you should determine which types of devices will require access and the mechanism of authentication/encryption that they support. This will drive the configuration of the system to support different user groups and security methods.

2.1 Recommendations

For a typical deployment, we recommend configuring at least one ESSID for the 3631 wireless telephones on a voice VLAN.

For PC's, configure additional ESSIDs. This traffic should be separated onto a secure VLAN.

3 DEPLOYMENT GUIDELINES

3.1 Virtual Cell

Meru Virtual Cell technology allows for zero-handoff as the wireless IP telephones roam through the wireless environment. This dramatically improves the quality and consistency of client roam times.

4 CONFIGURING THE MERU NETWORKS WLAN CONTROLLERS

Ensure that Basic controller configuration is complete including RADIUS authentication setup, if appropriate.

4.1 Security Configuration

Meru Networks supports the following 802.11 security mechanisms for wireless IP telephones:

- Clear (Open)

- WEP (64 or 128)
- WPA PSK (WPA Personal)
- WPA2 PSK (WPA2 Personal)
- WPA (WPA Enterprise with 802.1X)
- WPA2 (WPA2 Enterprise with 802.1X)

4.1.1 WPA2

Sample WPA2 security profile with 802.1X authentication and AES data encryption:

- L2 Modes Allowed - WPA2
- Data Encrypt – CCMP-AES
- Primary RADIUS Profile Name – *Select Primary Server*
- Secondary RADIUS Profile Name– *Select Backup Server*
- 802.1X Network Initiation – On
- MAC Filtering - Off

4.1.2 WPA

Sample WPA security profile with 802.1X authentication and TKIP data encryption:

- L2 Modes Allowed - WPA
- Data Encrypt – TKIP
- Primary RADIUS Profile Name – *Select Primary Server*
- Secondary RADIUS Profile Name – *Select Backup Server*
- 802.1X Initiation – On
- MAC Filtering – Off

4.1.3 WPA PSK

Sample WPA-PSK security profile with TKIP data encryption:

- L2 Modes Allowed – WPA PSK
- Data Encrypt – TKIP
- 802.1X Initiation – Off
- Pre-Shared Key – *specify Key Value*
- MAC Filtering – On (If this is on, MAC Addresses for phones must be defined in the MAC Filtering Permit list)

Note that you may enter the WPA PSK key as either a string or the hexadecimal representation of the string. Note that on the 3631 Wireless Telephones you also may enter the key in ASCII string or hex format.

4.2 VLAN Configuration

It is often desirable to separate voice packets from other data streams once the traffic enters the wired network. In the Meru solution, creating a VLAN entry in the controller and assigning it to the wireless telephone ESSID achieves this. This is an optional configuration component.

4.3 Deployment Modes

The Meru Networks Air Traffic Control system supports two modes of deployment: Virtual Cell and non-Virtual Cell. In Virtual Cell mode, all of the access points on the same channel will utilize a single BSSID. This allows the system to perform client handoffs between access points without the client devices needing to perform 802.11 or 802.1X re-association procedures to the new access point.

4.4 ESSID Configuration

The ESSID used by wireless IP telephones would be configured for Virtual Cell and assigned the appropriate security profile.

- SSID – *chosen_SSID_name*
- Security Profile name – *select_security_profile*
- SSID Broadcast – OFF
- Tunnel Interface Type – Configured VLAN Only
- VLAN Name – *chosen_vlan_name*
- Allow Multicast Flag - Off
- Silent Client Polling - On

4.5 Turn off A channels on SSIDs

Go to each ESSID used by the 3631 telephones, and select the ESS-AP Table tab (at top). Sort by Channel for all APs.

- *Chosen_SSID_name* – delete all A Channels (40)

This step removes all the A band from the 3631 SSIDs because the 3631 wireless telephones only use B/G.

5 AP CONFIGURATION

Short pre-amble should be turned off per AP for wireless IP telephones.

Go to Configuration, Wireless Interfaces. Sort by Channel. Select all **B/G Interfaces (Channel 6). Do NOT set this on the A interfaces (Channel 40).**

After all selections, select Bulk Update.
Select Short Preamble: Off
And Select OK.
The APs will reboot to process this change.